Amendment filed: January 13, 2005

Appl. No. 09/499,633 Art Unit 3621

Page 8 of 13

REMARKS

Claims 1-3 and 40-46 are pending in the present application. By this reply,

claims 4-39 have been cancelled and claims 40-46 have been added. Claims 1

and 40 are independent claims.

The specification has been amended to clarify the invention. Such

amendments do not add new matter and are fully supported by the original

disclosure, e.g., Fig. 2.

REJECTION UNDER 35 U.S.C. §103

Claims 1-4, 19-22, 24-26, 28-29 and 31-39 have been rejected under 35

U.S.C. §103(a) 1 as being unpatentable over Schneck et al. (U.S. Patent 5,993,498)

in view of Akiyama et al. (U.S. Patent 5,784,464). This rejection, in so far as it

pertains to the presently pending claims, is respectfully traversed.

Regarding independent claim 1, Schneck et al. is directed to providing an

access mechanism 114 at a user site 104 as shown in Figs. 1 and 5. The access

mechanism 114 receives data such as the packaged data 150 or 108 from a

distributor 102. The packaged data 150 may include encrypted access rules 116,

¹ Applicants treat the Examiner's statement that these claims are rejected under 35 U.S.C. §102(e)

as being anticipated by Schneck et al. in view of Akiyama et al., as a typographical error since the

entire discussion of the rejection obviously involves 35 U.S.C. §103(a), which is also cited in

paragraph 10 of the Office Action.

Amendment filed: January 13, 2005

Appl. No. 09/499,633 Art Unit 3621 Page 9 of 13

or the encrypted rules may be provided to the user separately as the package rules

152 as shown in Fig. 5. The data sent to the user is encrypted with a data-

encrypting key K_D, which is encrypted using a rule-encrypting key K_R. The rule

encrypting key K_R is calculated as a function of the validated serial number of the

system 100 or 101 (column 14, lines 36-40 of Schneck et al.). Thus, in Scheck et

al., the access mechanism 114 decrypts the data-encrypting key KD using the rule-

encrypting key K_R and the decrypted data-encrypting key K_D is used to access the

data.

In clear contrast, in Applicants' invention as set forth in claim 1, a digital

data playing device stores a digital data file downloaded from a PC in a data

storage medium, wherein the stored digital data file has been encrypted by steps

of:

1) Generating an encryption key including at least a serial number of the

digital data playing device and/or an ID number of the storage medium;

2) Transmitting said encryption key from the digital data playing device

to an encryption/download unit of the PC through a network; and

3) Enrypting by the PC the digital data file using said encryption key.

For instance, as shown in Figure 2 of the present application, the MP3

player 130 generates an encryption key based on at least the serial number of the

MP3 player and/or the ID number of a storage medium such as a disc 140. This

encryption key ("16 BYTES E_K") is transmitted from the MP3 player 130 to an

encryption/download unit 124 of the PC 120 via a network. The

Amendment filed: January 13, 2005

Appl. No. 09/499,633 Art Unit 3621

Page 10 of 13

encryption/download unit 124 encrypts the raw data received from the encryption/decryption unit 123 using the received encryption key ("16 BYTES E_K") and then transmits the encrypted data to the MP3 player 130 for storage. The MP3 player 130 decrypts the stored encrypted data using the same encryption key to reproduce the decrypted data for playing the data therein. These features of claim 1 are fully supported by the original disclosure, for example, see Figure 2; page 6, lines 20-25; page 5, line 27 of the original specification for a communication network between the PC 120 and the MP3 player 130.

Clearly, in Schneck et al., there is no feature of transmitting the encryption key from the digital data playing device to an encryption/download unit of the PC, encrypting by the PC the digital data using this encryption key, receiving by the data playing device the encrypted digital data from the PC, and decrypting the digital data using the same encryption key, as in Applicants' claimed invention.

Furthermore, there is no generation of an encryption key "including at least a serial number of the digital data playing device/or an ID number of the storage medium" (claim 1) in Schneck et al. In Schneck et al., the rule- encrypting key K_R is generated based on a serial number of the system 100 in Figure 1 or 101 in Figure 5. In the last Office Action, the Examiner makes a number of assertions regarding what is specifically taught by Schneck et al. regarding this claimed feature. But Applicants respectfully submit that these assertions are not supported by the actual disclosure of Schneck et al. For instance, the Examiner states on page 4 of the last Office Action that Schneck et al. teaches an encryption

Amendment filed: January 13, 2005

Appl. No. 09/499,633 Art Unit 3621

Page 11 of 13

key "generated by using unique IDs associated with the product distributed, its

storage medium, player device, end user, product publisher, and/or any

combination of these numbers". But there is no disclosure support for such an

allegation. One thing that Schneck et al. teaches is that the rule-encrypting key

K_R is generated based on a validated serial number of the system and that the

data-encrypting key K_D is different for each product (i.e., for each packaged data

108). If the Examiner were to maintain the accuracy of such assertions, the

Examiner should identify the specific portion(s) and/or element(s) that the

Examiner relies on to support his position.

Furthermore, Akiyama et al. does not overcome these deficiencies of

Schneck et al. since Akiyama et al. is directed to using a random number

generator to generate a random number and encrypting the random number,

which is then used to encrypt data. Akiyama et al. does not disclose at least the

above-noted features as recited in independent claim 1.

Regarding independent claim 40, Schneck et al. and Akiyama et al., either

taken singularly or in combination, do not teach or suggest a digital data playing

device which includes "a second encryption algorithm encrypting an initial

encryption key which has been generated based on the ID number of the digital

data playing device or the associated memory; a decryption algorithm decrypting

an encrypted digital data downloaded from a PC using said encrypted encryption

key". In Schneck et al., it is the rule-encrypting key K_R, which is generated based

on the serial number of the system.

Amendment filed: January 13, 2005

Appl. No. 09/499,633 Art Unit 3621

Page 12 of 13

Therefore, even if the references are combinable, assuming arguendo, the

combination of references would still fail to teach or suggest the invention as

recited in independent claims 1 and 40 and their dependent claims (due to their

dependency). Accordingly, all the claims are allowable over the applied references,

and the rejection must be withdrawn.

CONCLUSION

In view of the above amendments and remarks, the present application is in

condition for allowance. Issuance of a Notice of Allowance is thus respectfully

requested.

Should there be any outstanding matters that need to be resolved in the

present application, the Examiner is respectfully requested to contact Esther H.

Chong (Reg. No. 40,953) at the telephone number of the undersigned below, to

conduct an interview in an effort to expedite prosecution in connection with the

present application.

Applicant(s) respectfully petitions under the provisions of 37 C.F.R. §

1.136(a) and 1.17 for a two-month extension of time in which to respond to the

Examiner's Office Action. The Extension of Time Fee in the amount of \$450.00 is

attached hereto with the filing fee for the RCE.

Amendment filed: January 13, 2005

Appl. No. 09/499,633 Art Unit 3621

Page 13 of 13

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

P.O. Box 747

Falls Church, VA 22040-0747

(703) 205-8000

JTE/EHC/te:sld 0630-0981P